PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2003-005641

(43) Date of publication of application: 08.01.2003

(51)Int.CI.

G09C 1/00 H04L 9/08 H04L 12/28

(21)Application number: 2001-191559

(71)Applicant: NEC CORP

(22)Date of filing:

25.06.2001

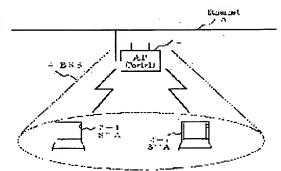
(72)Inventor: SHIMIZU MEGUMI

(54) METHOD AND APPARATUS FOR AUTHENTICATION IN WIRELESS LAN SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and an apparatus for authentication in a wireless LAN system which can concurrently achieve delivery of an encryption key for maintaining concealment between only parties performing wireless communication and an authenticating procedure and can simplify each authenticating procedure to the same AP (a base station) performed by a S TA (a mobile terminal) completing initial authentication after releasing the authentication.

SOLUTION: The STA searches whether a MAC address of the AP intending to perform the wireless communication exists in an AP information managing table maintained by the STA. If the MAC address does not exist in the AP information managing table, a request for authenticating a public key is transmitted to the AP. If the MAC address exists in the AP information managing table, a request for re-authenticating the public key is transmitted to the AP.



LEGAL STATUS

[Date of request for examination]

28.05.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3702812

[Date of registration]

29.07.2005

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

3 (19) 日本四条件庁 (JP)

許公報(A) 那特 ধ

(11) 特許出國公園由中 **特開2003-564**1

(P2003-5641A)

(43)公開日 平成15年1月8日(2003.1.8) (有無)、十二十二 5 J 1 0 4 5K033 640Z 300E 601C 601E 1/00 2605 H04L

> 640 300

2080 (51) Int.Q. H041

(全13月) 開水項の数18 01 整色整头 允

(11) 出版人 **停買2001**-191559(P2001-191559) (21)出版集中

平成13年6月25日(2001.6.25)

(22) 出版日

東京都港区芝五丁目7番1号 日本電気株式会社 新木 めへゆ 000004237 (72) 発明者

(74)代理人 100082835 以作件人

机大部形区芝五丁目7番1号 日本偏気株

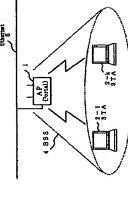
F ターム(事事) 5J104 AA07 AA18 EA08 EA19 KA02 **外班士 京本 貞樹 (外2名)**

KADS KAD6 NAD2 NA20 SRO33 AA08 CC02 DA01 DA19

(54) [発明の名称] 無様LANシステムにおける配配方法と認証投票

た暗号用の鉄配送と認証年頃の同時実現を可能とすると 共に、初回の酩飩を完了したSTA(移動端末局)に関 しては、怒耐解験後の同一AP(題地局)に対する2回 目以降の認証手順の簡略化を実現可能とする、無線LA 【袰題】無鉄通信を行う当事者関でのみ秘匿性を保持し Nシステムにおける認証方法と認証装置を提供する。

【解決手段】STAは、無額通信を行おうとするAPの ル内に存在するか否かを検索し、前配MACアドレスが 切配AP情報管理テーブル内に存在しない場合には、前 EA Pに対して公開機器位要水を行い、前配MACTド は、前配APに対して公開維再認証要求を行うことを特 MACアドレスがSTAの保持するAP情報管理テープ レスが粒的AP情報管理デーブル内に存在する場合に



ACアドレスが前記AP情報管理テーブル内に存在する おいて、STA (移動機末周)は、無線通信を行おうと ナるAP(基地局)のMACアドレスが析配STAの保 **种するAP情報管理テーブル内に存在するか否かを検索** し、前記MAC7ドレスが前記AP情報管理テーブル内 場合には、前配STAは前配APに対して公開蝦再認配 要求を行い、前配APは前配公開業再認配要求が妥当で 【職水項1】 無様LANシステムにおける認配方法に に存在しない場合には、前配STAは前配APに対して 公開顧認質要求を行い、 植配A P は前配公開顧認証要求 が妥当である場合には前記STAの認証を行い、前配M ある場合には前配STAの認配を行う、ことを特徴とす る無様LANシステムにおける昭在方法。

【静水項2】 前記AP情報管理テーブルは、前記ST Aが前配公開機関配要求を行って核公開機関配の名丁典 質の有るAPのMACTドレスを最新認証完了実績順に 保存することを特徴とする情水項1に記載の無線LAN システムにおける脳証方法。 【精求項3】 前記APは、自ちの秘密観であるAP秘 STA秘密機に対応する公開機であるところのSTA公 密載と、前記AP 秘密機に対応する公開機であるところ E明春であるところのAPユーザ証明者とを保持し、前 RSTAは、自らの鉛密機であるSTA粉密機と、前記 **頻像と、前記STA公開機を付した自らのユーザ証明者** ことを辞散とする諸水項1或いは精水項2の何れか1項 のA P公院徴と、村配A P公別機を付した自らのユーザ であるところのSTAユーザ証明書とを保持している、 こ記載の無額LANシステムにおける認証方法。

ーザ証明権を前記APに対して沿信するステップと、前 【時本項4】 前配STAが前配APに対して前配公開 **製怒配要求を行うステップは、公開機器配手頃によって** 常成され、前配公開機器低手順は、前配STAから前配 APに対して認配要求を行うステップと、前記認配要求 を受信した前記A Pから前配S TAに対して前記A Pユ ーザ証明書を送信するステップと、前記APユーザ証明 都を受信した前配STAが、前記APユーザ証明事を検 阻した後に前配APユーザ証明書に添付された前配AP 公開機を用いて前配STAューザ証明書を暗号化して暗 **学化STAユーザ証明書を作成し、前記暗号化STAユ** 記略号化STAユーザ取明物を受信した前記APが、前 記略号化STAユーザ証明書を前記AP級密観で復号化 して前記STAユーザ証明者を再生し、前記STAユー **ザ胚明書を検証した後に前配STAユーザ胚明書に添付** された前配STA公開鍵を用いて前配APが生成した共 通識を暗号化して暗号化共通機を作成し、前記暗号化共 意識を前記STAに送信して認証許可を通知するステッ プとから構成され、 前配階号/大共通機を受信した前配S TAが、前配暗号化共通機を前配STA絡密録で復号化 **つれ 杉町 共通戦 か 再生 し、 以降 の レッー 4 暗 早 力通信 に**

8

族共通観を使用する、ことを特徴とする請求項3に記載 の無様しANシステムにおける認証方法

戦器拡栗水を行う際に送受信されるMAC7 レーム内の フレームボディ街のAlgorithm Numberの値は、「0」又 【職女女5】 「村記STAが特配APに対して村配公開 は「1」でない在板の数「n」である、ことを特徴とす **る間水項4に記載の無線LANシステムにおける認在方**

Aの認証許可時に生成し発行した共通難とを、最新認証 し、前配公開機管理デーブルは前配A P が過去に移位件 と、験STAの前配STA公開館と、前記APが終ST 作可関に保持する、ことを特徴とする請求項5に記載の Fを通知した実績の有る机配STAのMACアドレス 【数水項6】 前配APは公開整管理アーブルを保持 無線LANシステムにおける認証方法。

女を必信した哲配STAのMACTドレスが前記APの。 【職水及7】 「新店STAが前記APに対して約記公開 って構成され、前記公開機再踢配手模は、前記STAか ら前記APに対して再認証要求を行うステップと、前記 再窓位要求を受信した前記APが、前記公開競再路配要 し、検索した結果、ff配STAのMACTドレスがff配 公開原管理アーブルに存在し、かり、IRMACアドレス に対応する公開機であるところの析配STA公開機を前 的公理教育理デーブルを冗保辞していることを確認した 場合には、前記APは、当抜STAに対して指定する新 たな共通観である新共通観を生成し、政新共通観を前配 STA公開銀で暗号化して暗号化筋共通観を生成し、飲 暗号化新共通観を前配STAに治信して認証許可を通知 するステップとから構成され、村配暗号化新共通観を受 信した前記STAが、前記暗导化新共通観を前記STA 的密膜で復歩たして哲的推共通難を再生し、以降のレッ 一ム暗号化通信に放新共通線を使用する、ことを特徴と **費再邸証要求を行うステップは、公開戯再認証手頃によ** する簡求項6に記載の無数LANシステムにおける認証 保持する前記公開整管理テーブル内に存在するか検索

単序的信服状を行う際に必要信されるMACフレーム内 【簡求項8】 「動配STAが簡配APに対して動配公開 と「1」と「n」でない任我の数「m」である、ことを ¥徴とする糖水項7に記載の無線LANシステムにおけ のファームボディ筋のAlgoritha Namberの値は、「0」

【臍水項9】 無様LANシステムにおける認証装置に 35vで、無砂道信を行おうとするAP(基地局)のMA P情報管理デーブル内に存在しない場合には、前記AP に対して公開戦略配要求を行い、 ffilEMACアドレスが 析記AP情報管理アーブル内に存在する場合には、析記 Cアドレスが自身の保持するAP情報管理テープル内に 午在するか否かを複称し、 fdEMACアドレスが前記A APに対して公開機再認証要求を行うSTA(移動増末 €

局)と、前記STAからの前記公路機関回収水あるいけ 前記公路機再路回要水が設当である場合には前記STA の路配を行う前記APと、全価えることを特徴とする結

様LANシステムにおける際配装庫。 【酵水塩10】 前ZAP債候管理テーブルは、前配S TAが前型公開機能配要水を行って様公開機能配の完了 実種の有るAPのMACアドレスを最新認配給了実績の に保存することを特徴とする間水項のに配慮の無線LA Nシステムにおける認配装置。

[請求項12] 前記STAが前記APに対して前記公 に対して認証要求を行い、前記認証要求を受信した前記 的密盤と、析配A P級密盤に対応する公開鍵であるとこ ろのAP公開瞭と、前配AP公開瞭を付した自ちのユー 析記STAは、自らの秘密機であるSTA秘密機と、前 祀STA秘密機に対応する公開機であるところのSTA 公開機と、前配STA公開機を付した自らのユーザ証明 る、ことを称数とする請求項9数いは請求項10の何れ 開機路配要求を行う場合には、前記STAから前記AP APから前記STAに対して前記APューザ配明書を送 析記APユーザ証明書を検配した後に前記APユーザ証 明書に添付された前配AP公開機を用いて前配STAユ **一ず証明書を暗号化して暗号化STAユーザ証明書を作** 成し、前記略身化STAューザ配明書を前記APに対し て送信し、前記暗号化STAユーザ証明書を受信した前 記APが、前記暗号化STAユーザ証明者を前記AP総 密機で復身化して析配STAユーザ証明審を再生し、前 記STAユーザ証明書を検証した後に前記STAユーザ 証明書に添付された前記STA公開鍵を用いて前記AP **前記暗号化共通機を前記STAに送信して認証許可を通** 知し、前記暗号化共通機を受信した前記STAが、前記 暗导化共通機を前記STA物密離で復身化して創配共通 最を再生し、以降のフレーム暗号化通信に該共通殿を使 用する、ことを特徴とする請求項11に記載の無級LA **が証明書であるところのAPューが証明者とを保持し、 信し、前記APユーザ証明書を受信した前記STAが、** が生成した共通轍を暗号化して暗号化共通轍を作成し、 替であるところのSTAユーザ証別書とを保持してい か1項に記載の無談LANシステムにおける認証装置。

「鶴水県13」 前記STAが前記APに対して前記公 副職総記要求を行う際に送受信されるMACフレームが のフレームボダイ部のAlgorith Numberの値は、「0」 又は「1」でない在物の数「n」である、ことを特徴と する陽水県12に配象の指摘LANンステムにおける総 指指層

Nシステムにおける認配装置。

【韓水項14】 前記APは公開線管理テーブルを保存 し、前記公開線管理デーブルは前記APが過去に認証許可を通めした実績の有る前記STAのMACアドレメ と、様STAの前記STA公開機と、前記APが核ST

Aの認証許可時に生成し発行した共通職とな、最新認証 中国現に保持する、ことを特徴とする職状項13に配載 の無線LANシステムにおける認証装置。

Pに対して再級胚要求を行い、前配再認証要求を受信し 音理テーブル内に存在するが複索し、検索した結果、前 存在し、かつ、飲MACTドレスに対応する公開機であ は、当該STAに対して指定する教たな共通機である新 RSTA秘密機で復身化して前配新共通機を再生し、以 [新水項15] 前記STAが前記APに対して前記公 R蘇再認証要求を行う場合には、前配STAから前配A と前記APが、前記公開線再認証要求を送借した前記S 「AのMACアドレスが柏配APの保存する柜配公開職 RSTAのMACアドレスが前配公開機管理テーブルに るところの析配S T A公開機を前配公開機管理テーブル 共通鍵を生成し、放新共通鍵を前記STA公開機で暗号 **代して暗号化新共通機を生成し、紋暗号心筋共通機を前** 記STAに送信して認証許可を通知し、前記暗号化新共 高級を受信した前記STAが、前記時号化新共通機を前 降のファーム暗号化通信に放射共通機を使用する、こと を停倒とする間水項14に記載の無線LANシステムに 内に保持していることを確認した場合には、 が配AP **おける認証装置**

【韶本項16】 「新RSTAが創版APに対して前限公 解験再級庇要水を行う際に過失信されるMACファーム 約のファームボディ語のAlgorith Numberの値は、

カのフレームボディ群のAlgoritha Nuberの値は、 「0」と「1」と「n」でない任義の数「m」である、 ことを特数とする間末項15に配象の指数LANンステ

ムにおける認配装置。 【発明の詳細な説明】

[0001]

「発明の属する技術分野」本発別は無線しANシステムにおける認成方法と認配装置に関し、特にゲータを確与化して無終温信する無線LANシステムにおいて、無線通信を行う当事者間でのみ認確性を保持した確与用の糖配法と認配の同時実践を可能とする、無線LANシステムにおける認配方法と認配法を認定が表と認配業置に関する。

[0002]

【従来の技術】無数LAN(Local Area Network:ラン)ンステムにおいては、遊牧信するデータの必服告を 保存するために、遊牧信するデータフレームの語母化が 必須の条件となってきている。 [0003] 無線LANシステムにおける暗号化方式については、これまでIEEE (Institute of Electrica land Electronics Enginers:米国、電気/電子技術音協会)802委員会を中心として標理化の複形が進められてきており、その精理仕様であるIEESの2.1においては、無線LANにおける無線区間の暗号化及び窓匠の方式の1つとして、Stared & で (共通機)認紅方式が採

[0004] Shared Key方式においては、図1に示すよ

うな無線LANの基地局としてのAP(Access Point: アクセスポイント)1と移動場来局としてのSTA(St ttion:ステーション)2とが、通信相手体に互いに保 神子をことのできる1種類の共通線を使用する。又は1 種類の共通線を保持していない場合には、両者共通の離 情報として4種類の共通線を保持しておき、フレーA用 身化返信を行う際には4種類の共通線を保持しておき、フレーA用 身化返信を行う際には4種類の共通線を保持しておき、フレーA用 機を撮欠して使用するようになっている。しかし、暗号 代用の販売が基出版しては、IEEEB02.11には定義さ れておらず、実験依存しなっている。

【0005】Shared Key方式における認証年頃について、<u>図10及び図11</u>を参照して説明する。

[0006]<u>図10</u>は、Shared Key方式における認証年 優を示す図であり、<u>図11</u>は、Shared Key方式の認証年 優において送受置されるフレームフォーマットのフレームボディ部を示す図である。 【0007】<u>図10</u>において、AP1に対してShared K eyお式による窓面要求を行うSTA2は、AP1に対し て窓配フレーム1を送信する(ステップS1)。 器配フレーム10フレームボディ街は、<u>図11</u>の(1)器配フレーム10アレームボディ街は、<u>図11</u>の(1)器配フレーム10デオ形式となっており、Algoritha Number (アルゴリズム番号) 11—1—1を「1」とし、Iran saction Sequence Number (トランデクションシーケン ス番号) 11—1—2を「1」としたフレームとなっている。なお、Shared Keyが式における認証等には、Algoritha Number 11—1—1~11年に「1」 であると座鏡されている。

[0008] ステップS 1でS TA 2から臨屆東本登録 信じたAP 1は、認証フレーム2を用いてGallenge Te お(チャレンジネスト) というランダムなビット列を STA 2に対して選手を (ステップS 2)。既 アレーム2に示す続大を なっており、Algoritha Naber 11ー2ー1は対策の通 り「1」であり、Transaction Sequence Naber 11ー 2ー2は「2」で、Gallenge Text element (チャレンジテネトエレメント) 11ー2ー4にGallenge Text element (チャレンジテネトエレメント) 11ー2ー4にGallenge Text を挿入したフレームとなっている。 40009] ステップS 2でAP I から影配フレーム2 を受信したSTA2は、AP I から受信したChallenge Textと、原たballenge Textに対するCRC2(Cyclic Redundency Code 22bits)集出結果に指当するCRC2(Citregrit f Check Value : インテグリティキェックバリュー)に 対して、共通機の1つで暗号化を行う(ステップS 3)。そして、暗号にしたballenge TextとICV を、使 用した共通機の整備報であるIV (Initialization Vector エーンケライゼイション・ベクター)と共に、認在 フレーム3を用いてAP Iに対して送信する(ステップ S4)。認在フレーム3は、図11の(3)数征フレー A3に示す形式となっており、Algoritha Numbert 11— 3—11は前述の通り「1」であり、Transaction Sequen

ce Number 11—3—2は「3」で、[V11—3—3、 Chellenge Fext element (研号化したChellenge Fext) 11—3—4、[CV 11—3—5を付加したフレームと

0 [1] 730, Transaction Sequence Number 11-4 P 1 は、安信フレーム内政情報(IV111—3—3)か 国11に示したStatus Code 11-1-9、Status Cod Code 11-4-9は、フレーム受信成功の可否などを [0010] ステップS4で認証フレーム3を受信した 3.それに対応する共通観を用いて受信ファームの暗号C 5) と彼号結果から算出したICM の一致と、復号結果か 5得られる平文とステップS2で送信したChallange Te ttとの一般を確認した場合には (ステップS 5 で一般を 確認した場合)、 総駐フレーム4をSTA2に対して治 **省して認証完了を通知する(ステップS6)。認証フレ - 44は、図110 (4) 認用ファー44に下す形式と** なっており、Algoritha Marber 1 1ー4ー1 は長浴の通 e 11-2-9, Status Code 11-3-9及UStatus 4-2は「4」で、Status Code (ステータスコード) おを復号化し、受信フレーム内ICM (ICM 11—3— 11-4-8を杆加したファームとなっている。 なお、 画信相手に通知するための信仰フィールドである。

[0011]以上の軟件により、Shared Ker方式における路底手間が終了し、以後、STA2とAP1間で共通機を用いたフレーム暗号化道値が行われるようになって、

【毎明が解決しようとする課題】第1の例として上述した確確理ませーバを利用したシステムでは、予め移動端末島の情報を贈管理サーバを発用したシステムでは、予め移動端末島の情報を贈管理サーバに登録しておくものであり、糖品送手頭と認証手頭が投離されることにより、暗号化を半り認証手頭が接端なものとなるという欠点を有してい

[0014] また、第2の房として上述した韓国治フルゴリズムを用いた総国年間においては、通信を行う当事首的でのお総原年後になっては、通信を行う当事首関でのみ総原任を保存した韓国法と認証を国際に行う

9

9

存配2003—5641

ことが可能となるが、その認証手間が搭縁となり度算に 多くの時間を要するものとなっており、無数価値環境の 問題などによって適信が絶たれた際の認証解除時におけ る再度の認証手類実行時にも、初回の認証時と同一手模 を踏むこととなり、本来のデータ通信以外のオーバーへ ッドトラヒックを増大させてしまうという欠点を有して

【0015】本部別は上述した事情を改善するためになされたものでもり、本知別の目的は、無能価値を行う当事者間での分級医性を保持した時号用の鍵配送と認証手類の同時実現を可能とすると共に、初回の認証を完了したSTA (移動域共局)に関しては、認証解除後の同一AP (基地局)に対する2回目以降の認証手順の関略化を実現可能とする、無線LANシステムにおける認証方由と認証素を整件することにある。

[0016]

「課題を解決するための手段」本説明の無数LANシステムにおける認匹方法は、無数LANシステムにおける 認成方法にないて、STA (移動地末局)は、無線通信 を行おうとするAP (基地局)のMACアドレスが前記 STAの保持するAP情報管理テーブル内に存在するか 否かを依然し、前記MACアドレスが前記AP に保健管理 テーブル内に存在したい場合には、前記STAは前記AP Pに対して公園機器配要求を行い、前記AP は前記AP い、前記MACアドレスが前記AP は保健管理 ト・、前記MACアドレスが前記AP は保管理テーブル内 に存在する場合には、前記STAは前記AP に対して公 別議再級配要求を行い、前記STAは前記AP に対して公 別議再級配要求を行い、前記STAは前記AP に対して公 別議再級配要求を行い、前記STAは前記AP に対して公 別議再級配要求を行い、前記STAは前記AP に対して公 会場とするる場合には前記STA の認証を行う、こと を希徴とする。

【のの17】また、前配AP情報管理ナーブルは、前配STAが前配公服機能配要求を行って様公服機能配の 子実績の有るAPのMACアドレスを表施認配出了実績の指したので、アンスを表施認配出了実績の再るAPのMACアドレスを表施認配出了実績層に保持することを全世とする。

[0018]を与に、前記APは、自ちの総保職である AP総を建と、前記APが総裁に対応する公開職である ところのAP公開職と、前記AP公開職を付した自らの ユーザ配明事であるところのAPユーザ配明事とを保持 し、前記STAは、自らの総保機であるSTA総総機 と、前記STA総総職に対応する公開職であるところの STA公開機と、前記STA公開機を付した自らのユーザ配明事とあるところの STA公開機と、前記STA公開機を付した自らのユーザ配明事ともるところのSTAユーザ配明事とを保持している、ことを特徴とする。

【0019】また、前記STAが前記APに対して前記
公開線認証要求を行うステップは、公開線認証手項によって構成され、前記公開線認正手項は、前記STAから 前記APに対して認証要求を行うステップと、前記認証 要求を受信した前記APから前記STAに対して前記A Pコーザ証労争を送信するステップと、前記APコーザ 配別事を受信した前記STAが、前記APコーザ

を検距した後に加配APコーザ配列等に添付された前配AP公開機を用いて前配STAコーザ配列等を酵号化して酵号化STAコーザ配列等を酵号化とて酵号化STAコーザ配列等を酵号化とで酵号化STAコーザ配列等を対して送信するステップと、前記時号化STAコーザ配列等を対してが開立APが対面APが設置を発生してが配置とれてが配置とれるコーザ配列等を再生し、前面STAコーザ配列を表して表面を終めてASM機を開いて前配ATAが設置を発生して表面を発展して表面を対した表面をを時配STAに送信して表面を対して対面を対して表面を対して対面を対して対面を対して対面を対して対面等化は温度を対して対面等の表面が、前記時号化共温度を対配STASの意型が高温にあた、前型は分化共温度を対配STASの意型が多ステップとから構成され、対配等分化共温度を対配STASの意型が高温にあた、前型は多数を表し、以降のフィーは暗号化

【0020】さらに、前配STAが前配APに対して前 E公開職窓距線水を行う際に送受信されるMACフレー Aやのフレームボディ部のAlgoritha Nadorの値は、 「0」又は「1」でない任意の数「n」である、ことを「0」又は「1」でない任意の数「n」である、ことを

特徴とする。 [0021]また、前記APは公開機管理テーブルを保存し、前記公開機管理テーブルは前記APが過去に認証 許可を通知した実績の有を前記STAのMACアドレス と、該STAの前記STA公開機と、前記APが終ST Aの認証許可時に生成し発行した共通機とを、最新認証 許可順に保持する、ことを特徴とする。

のフレーム暗号化通信に放新共通験を使用する、ことを 記A Pの保持する前記公別業管理テーブル内に存在する が検索し、検索した結果、前配STAのMACTドレス 数を前記公開銀管理テーブル内に保持していることを確 認した場合には、前配APは、当校STAに対して指定 する新たな共通鍵である新共通機を生成し、紋新共通機 を前記STA公開機で暗号化して暗号化新共通機を生成 し、眩暗号化新共通離を前配STAに送信して路配許可 を通知するステップとから構成され、前配路号化新共通 **建を受信した前記STAが、前記時号化新共通機を前記** STA的密鞭で復身だして村配を共通機を再生し、以降 【0022】さらに、 哲配STAが的配APに対して樹 記公開義再認証要求を行うステップは、公開鏡再認証手 頃によって構成され、前配公開廰再路配手頃は、前記S 再認問眼状を治信した哲能STAのMACT ドレスが制 が析記公開機管理テーブルに存在し、かり、核MACア ドレスに対応する公開鍵であるところの前配STA公開 と、前記再級配要求を受信した前記APが、前記公開側 TAから前記APに対して再認証要求を行うステップ

年費とする。 [0023] また、相配STAが制配APに対して利配S里藤東認能職夫を行う歴に治安僧されるMACファームかのファームがディギのMaoritha Nadorの値は、

10」と「1」と「n」でない任頼の数「m」である、

ことを転散とする。

【0024】本発明の無線LANシステムにおける認証 装置は、無線LANシステムにおける認配装置において、無線通信を行おうとするAP(基地局)のMACアドレスが自身の保神するAP情報管理テーブル内に存在するか否かを検察し、前配MACアドレスが耐配AP情報管理テーブル内に存在したい輩台には、前記APに対して公照機能配要求を行い、前配MACアドレスが耐記AP情報管理テーブル内に存在する場合には、前記APに対して公照機等現テーブル内に存在する場合には、前記APに対して公開機等程度である。 を、前記STAからの前記公服機能配置要求あるいは前記 公服機等短配要求が投当である夢台には前記STAの認 配を行う前記APと、を備えることを特徴とする。

100251また、「耐力AP権権管理ナーブルは、耐力 STAが研究の機能の形象を行って終め開撃的の光 実験の有るAPのMACアドレスを機能的配売了実験 関係保存することを検験とする。 【0026】さらに、前記APは、自らの総の職であるAP総の職と、前記AP総の職に対応する公職職であるところのAP公職職と、前記AP公職職を付した自らのコーザ監明権であるところのAPコーザ監明権とを保持し、前記STA総の職に対応する公職職であるSTA総の職と、前記STA総職職を付した自らのコーザ監明権であるところのSTA公職職を付した自らのコーザ監明権であるところのSTAコーザ配明権とを保持している、ことを特徴とする。

を作成し、前記語号化STAユーザ証明者を前配APに 【0021】#14、型配STAが動配APに対して動配 Pに対して認証要求を行い、前記認証要求を受信した前 RAPから析配STAに対して前配APユーザ証明書を Aユーザ証明書を暗号化して暗号化S TAユーザ証明書 対して送信し、前記簿号化STAューザ証明権を受信し し、枸配STAユーザ証明書を検証した後に前配STA ユーザ証明毎に添付された前記STA公開機を用いて前 EAP が生成した共通機を暗号化して暗号化共通機を作 前記共通鏡を再生し、以降のファーム暗号化通信に該共 公開機器監要求を行う場合には、前配STAから前配A 45、前記APユーザ証明書を検配した後に前記APユー が配明書に数付された前記AP公開機を用いて前記ST た前記AP が、前記暗号化STAユーザ証明者を前記A 成し、前記暗号化共通轍を前配STAに送信して認配幹 が、前部番子化共通機を削配STA笏密機で復与化して 可を通知し、前配暗号化共通鍵を受信した前記STA 送信し、前記APユーザ証明書を受信した前記STA P的密盤で復号化して前記STAユーザ証明書を再生 通鍵を使用する、ことを特徴とする。

【0028】さらに、乾悶STAが着配APに対して前記会職総配原来を行う際に治安信されるMACソームなのファームボディ部のAlgorith Naberの値は、「0」又は「1」でない石物の数「n」である、ことを「0」又は「1」でない石物の数「n」である、ことを

等徴とする。 [0029]また、前記APは公開整管理アーブルを保 等し、前記公開線管理アーブルは前記APが過去に認証 許可を通知した実績の有る前記STAのMACアドレス と、様STAの前記STA公開機と、前記APが模ST Aの認証許可時に生成し発行した共通機とを、最新認証 許可順に保持する、ことを特徴とする。

アルに存在し、から、核MACアドレスに対応する公開 難であるところの何配STA公開機を何配公開験管理予 ープル内に保存していることを確認した場合には、前記 APは、当該STAに対して指定する新たな共通機であ **る新共通鍵を生成し、紋新共通機を前配STA公開瞭で** 暗号化して暗号化新共通概を生成し、核暗号化新共通概 を前記STAに送信して認証許可を通知し、前記暗号化、 所共通機を受信した前配STAが、前配暗号化新共通録 [0030] さらに、前配STAが前配APに対して前 RAPに対して再級配要求を行い、前配再認配要求を受 信した析記APが、析記公開競再認証要求を送信した析 RSTAのMACアドレスが前記APの保持する前記公 果、枸杞STAのMACアドレスが前配公開整管理テー R公開鏡再認証要求を行う場合には、前記STAから前 現態管理テーブル内に存在するか境祭し、検索した結 を前記STA物の機で復与化して前配筋共通機を再生 い、以降のファーム暗号化通信に該新共通機を使用す

る、ことを称換とする。 [0031]また、前配STAが前配APに対して前配公服職再認取果を行う原に送受信されるMACフレーム内のフレームがディ部のMgaith Nuberの値は、「0」と「1」と「n」でない缶敷の数「m」である、ことを称数とする。

- CATTRON 1 3。 [0032] [発明の実施の形態] 大に、本発明の実施の形態につい

て図画を参照して説明する。 [0033] 図1は本語明の指摘LANシステムにおける数のお指揮し書紙形能をデナプロック図である。

ice Set : 基本サービス・セット) 4と言う。 [0035] BSS4内におけるAP1は、各STA2 がAP1に同致するための情報を含むBescon (ビーコン) フレームを、風類的にBSS4内にプロードキャスト諸信し、当該Besconフレームを受信したBSS4内の各STA2は、通信開始時にAP1に対して認証要求を行い、AP1により認証許可を受けた後、AP1への第行い、AP1にか認証許可を受けた後、AP1への第 <u>®</u>

異処理を完了することにより、AP1との通信を行うこ とが可能となる。また、Infrastructure方式における日 SS4内の合STA2は、STA2関連信仰においても AP 1を介した通信を行う。

[0036] また、図1におけるAP1は (portal) と なっているが、Portalとは、IEES02.11以外のLANブ とを示しており、基地局としてのAP1とEthern e t (聖政商標) (イーサネット (圣政商標)) 5 など の有様LANとの接続を可能にした基地局であることを ロトコルとのブロトコル投換機能をAP1に付加したこ 示している。

無線区間の暗号化及び路配の方式として、Shared Key方 式(共通襲怒証方式)とは異なり、主として秘密競と公 開戦を用いた認証方式を採用している。従って、Shared [0037] なお、<u>図1</u>に示した実施の形態は、IEEB80 2.11に勧牲したものかももが、 存実街の形態においては Key方式と区別するために、本実施形態における観覧方 式を公開機器配力式と便宜的に呼ぶこととする。

[0038] 太に、<u>図2を</u>参照して、AP1とSTA2 の詳語解成について数別する。 [0039] <u>図2</u>は、APとSTAの一例を示す体格プ ロック図である。 [0040] <u>図2</u>において、上段のブロック図がAP1 であり、下段のブロック図がSTA2である。

9-12上位レイヤとのインターフェースであるところ 数LANカード19-2は、同一の構成を備える。 従っ [0041] AP1は、図2に示す無数LANカード1 の上位レイヤインターフェース 1.7~1を介して、TC P/I P (Transport Control Protocol/Internet Prot ocol) や各種アプリケーションなどの上位プロトコル処 理を、基地局域末本体18にて実現するものであり、S TA2は、四2に示す無数LANカード19-2と上位 フイヤンのインターフェースであるところの上位ワイヤ インターフェース17―2を介して、AP1と同様な上 何プロトコルも断め、ノート数ペーンナルコンピュータ [0042] <u>図2に示す無数</u>LANカード19—1と無 て、無数LANカード19において同一の構成甲兼に対 **応するものは、個一の参照数字または符号を付しておく** などの移動機末本体20によって実現するものである。

層でのアクセス制御を行うIEE5302.11 MACプロトコル処 理的14と、MAC層での認証処理などの上位レイヤ処 [0043] <u>図2に示す無</u>線LANカード19 (19一 1及び19-2)は、無線区間でのフレーム送受信を行 理を、内臓するCPUとメモリ16によって実現する上 位レイヤ処理部15と、上位レイヤ処理部15が使用す (Physical Layer: 物理層) プロトコル処理部13と、 MAC (Wedital Access Control : 媒体アクセス勉強) う無線機断12と、変復観処理を行うIEE5802.11 PHY るメモリ16とから構成されている。 ものとする。

1

c対して認証を要求する際に、STA2とAP1間で送 [0044] 女に、<u>図3を</u>毎開して、STA2がAP1 を信されるMACフレームについて説明する。

[0045] <u>図3は、昭応東水</u>郷にAPとSTA間で送 トに従うMACフレーム30-1が、AP1とSTA2 (MACヘッダー) 30-2と、FrameBody (フレーム ドディ)30-3とFCS (Frame Check Sequence:フレ - ムチェックシーケンス)30-4とから構成されてい **1、図3に示す1距B02.11のMACフレームフォーマッ** 関で交換され、MACフレーム30—1は、MAC Header を信されるMACフレームの構成を説明する図である。 [0046] STA2のAP1に対する認証要求時に

leader 3 0 — 2 は、各種フレームタイプや制御情報を示 Prame Control (77-427-61-1) 30-11 ノ)30―12のフィールドと、フレーム设信先アドレ 30—13のフィールドと、フレームの液菌 元アドレス 1のフィールドと、BSS4の類型情報を示すBSID 3 0—15のフィールドと、ファーム送信贷を示すSequen [0041] そして、Infrastructure方式におけるMAC のフィールドと、送信先がピジーである場合に送信符機 を示すSA(Source Address:送信元アドレス)30—1 Se Control (ソーケンスコントロール) 30-16のフ スを示すDA (Destination Address : 送信先アドレス) を行うための時間を定義するDuretion (デュレーショ イールドから解説される。

[0048] フレーム送信時、<u>図2</u>に示すIEEE802.11 N ることにより、<u>図3に示すようなIEE802.11 MACプロト</u> にプロトコル処理的14では、上位レイヤ処理部16か 3に入れてカプセル化し、送信要求情報から作成したMA 当版MAC Header 3 0 - 2 とPrameBody 3 0 - 3に対する コルに従うMACフレーム30―1への役換を行う。 続 いて<u>図2</u>に示す1EEE802.11 PHYプロトコル処理的13で は、当該MACフレーム30—1に対する質糊処理を行 い、無線機断12を超て当成MACフレーム30—1を 5の送信要求フレームを、図3に示すPremeBody 30ー iS 30—4としてFrameBody 30—3の後ろに付加す C. Header 3 0 — 2 をPrameBody 3 0 — 3 の前に付加し、 AC32 (Cyclic Redundancy Code 32bits) 算出結果を、 空間上に送出することにより、送信処理が完丁する。

【0049】フレーム受信時、<u>図2に示すIEEB802.11 M</u> ICプロトコル処理的14では、無線機的12を超てIEEE 302,11 PNPプロトコル処理部13にて復調処理を行った 結果として受信したMACファーム30―1に対してCK 32 の計算を行い、受信フレーム内のFCS 30ー4の値 FCRC32 算出結果とが一致する場合には、NAC Header 3 い、FrameBody 30-3の部分を上位レイヤ処理断15 0-2の内容の解析と受信フレームに対する処理を行

【0050】女に、図4及び図5を伊服して、本実植形

なの重要な構成要素としての公開機管理テーブル及びA P情報管理アーブルにして、代明中も。

[0051] 四4は、APが保持する公開整管理テープ ルを説明する図であり、図らは、STAが保持するAP 情報管理テーブルを説明する図である。

[0052] AP1は、<u>図4</u>に示す公開整管理テーブル 16内に保持している。公開整管型テーブル40は、A P 1 が過去に本発明の公開難認証において認証許可を行 った実績の有るSTA2のMAC層の物理アドレスやも (STAのMACアドレス) 40—1の相と、当該ST 40-2の欄と、AP1が陽低許可時に当該STA2に AP 1は公開鐵管理テーブル40の各行を、STA2の 40を、<u>図2に示す無様LANカード19―1のメモリ</u> なして銘作した共通概を保持するShared Key(シェイー るところのMACアドレスを保持するSTA Mac Address A 2 の公開職を保持するPublic Key (パブリックキー) ドキー) 40-3の値とから禁収されている。そして、 最新認証許可順に登録する。

モリ16内に保持している。AP情報管理テーブル50 るAP MAC Address (A PのMACアドレス) 50-1の 種から構成されており、STA2はAP情報管理テープ は、STA2が本発明の公開難認証を要求して嫁公開機 ル50の各行を、AP1の最新路配完了実績限に登録す [0053] STA2は、図5に示すAP情報管理テー ブク50を、図2に小十舗装LANカード19―2のメ 路前の狛子安被の有るAP1のMACアドレスを保存す

ープル40~の情報登録時には、登録済みのSTA MAC ad Cアドレスが存在する場合には、登録内容の情報更新と 共に公開整管理テーブル40の先頭の行へ当政情報を移 動する。また、本発明の公開難器配完了後のフレーム暗 号化通信の実施毎に、AP1は公開競管理テーブル40 のSTA MAC address 40-1の検索を行い、通信相手の STA2の管理情報を公開職管理テーブル40の先頭の 行へ移動することにより、通信機会が新しい通信相手の 管理情報ほど管理テーブル上位に位置付けることで、公 開業管理テーブル40が限界型の数に強し、新規情報型 級が不可能となった場合には、公開験管理テーブル40 内で最も下位に位置する通信機会の最も古い通信相手の **【0054】AP1は、図4にて説明した公開銀管理予** dess 40-1の核紫を行い、既に密吸液みの同一MA 管理情報を削除することで対応する。

[0055] また、STA2はAP1と同様に、<u>図5</u>に は、数数内容の情報更新と共にAP情報管理テーブル5 0の先頭の行へ当該情報を移動する。また、本発明の公 A 2 はA P 情報管理デーブル 5 0 のAP LAC address 5 0 開棄認証完丁後のフレーム暗号化通信の実施毎に、ST r 税助した A P 信候指型 アーブグ 20 への信仰を受辱に は、昼殿済みのAP MAC address 5 0 — 1 の複素を行い、 既に型穀済みの同一MACアドレスが存在する場合に

—1の検索を行い、通信相手のAP1の管理情報をAP アク上位に位置付けることで、AP信機管理アーブグ5 0 が段界登録数に強し、新規情報登録が不可能となった 場合には、AP情報管理テーブル50内で最も下位に位 り、通信機会が新しい通信相手の管理情報ほど管理テー 置する通信機会の最も古い通信相手の管理情報を削除す 育権管理テーブル50の先駆の行へ移動することによ られたななける。

[0056]太に、図8、図2、図8、図8を参照し い、本戦権形類の動在にして、政政する。

(ナなわち、AP1成いはSTA2) との関係、及び保 ているものとする。そして、当該ユーザ配明書は、認証 育者自身の正当性を証明可飽である、という条件を前提 [0057] 本東極形態においては、図1に示した無数 LANシステムの、基地局であるAP 1と移動基本局で basta2は、共に、自らの秘密観とそれに対応する 公開鏡、及びIG公開競を添付したユーザ証明書を保持し 集関に代表される第三者によって、公開館とその保有者 とするものとする。以下では、ユーザ証明者はデジタル ューザ証明書を意味するものとする。

[0058] <u>図1</u>におけるSTA2がAP1を介しての。 無核通信を行おうとする場合には、STA2は先ずAP 1に対して、本発明の公開敷認証要求を送信することか い配給する。

[0059] STA2は公開機関范開始時に、認証要求 先のAP1のMACTドレスを用いて図5に示したAP 育な管理テーブル 5 0 PyのAP MAC Address 5 0 — 1 の換 P 1 のMAC7ドレスが存在しない場合には、初回の認 **位要求として図612示す公開敷認証年収を行い、認証要** 状先AP1のMACアドレスが存在する場合には、過去 に当該AP 1との公開機路配の完丁実績が有る場合であ るため、再認証として、<u>四3</u>に示す公開健再認証手順を 常を行い、AP情報管理アーブル50内に認配要求先A

[0060] 先ず、初回の認証要求としての公認職認証 <u>827</u>は、公開難認配手頃において送受信されるMACフ [0061] <u>図句</u>は、公開鍵認証年限を示す図であり、 年頃について、図6及び図2を参照して説明する。

ノーオのレフー 4 共 上 本 (区3 の FranceBody 3 0 ー

sr (アルゴリズム毎号) 70-1-1を「n」とし、fr [0062] <u>図6</u>において、AP1に対して公開戦協配 ファーム61のファームボディ形は、図7の(1) 略雨 ンス毎号) 70-1-2を「1」としたフレームとなっ 年間による認証要求を行うSTA2は、AP1に対して 8位フレーム61を送信する(ステップS61)。 80位 フレーム 6.1 に永十形式となっており、Algoritha Mab unsaction Sequence Number (トランザクションシーケ ている。なね、公開敷認証手順における認証時には、Al çoritha Number 7 0 — 1 — 1 ~ 7 0 — 4 — 1 は特に 3) を示す図である。

【0063】 ステップS 6 1 でSTA 2から公開機関配 要求を受信したAP1は、認証フレーム62を用いてA P1の保持するユーザ証明書をSTA2に対して送信す (2) 認用ファーム62に水上形式となっており、Algo rithm Number 70-2-1は前述の通り「n」であり、 る (ステップS62)。 認証フレーム62は、殴1の

で、APのユーザ配明470-2-3にAP1の保持する ユーザ胚明書(ユーザ配明春に付随するAP1の公開機 fransaction Sequence Number 70-2-21 12, をも付したもの) を挿入したファームとなっている。 【0064】ステップS62でAP1から認能フレーム 62を受信したSTA2は、AP1から受信したAP1 のユーザ証明**律**の内容を検証して、AP1のユーザ証明 春の検証結果に問題の無いことを確認すると、AP1の ューザ証明書に添付された公開録を用いて、STA2の STA2のユーザ位明春に付配するSTA2の公開機と 共に、怒腔フレーム63を用いてAP1に対して送信す 保存するユーが証明者の暗号化を行う (ステップS6 3)。そして、暗身化したSTA2のユーザ原野物を、

(3) 既開ファーム63に形十形式となっており、Algo

Transaction Sequence Number 70-3-211 [3]

る (ステップS64)。 認備フレーム63は、殴1の rith Nuber 7 0 — 3 — 1 は哲路の踊り「n」であり、

【0065】ステップS64で認証フレーム63を受信 で、APO公開館で暗号化したSTA のユーザ証明を20-3-3名件払したソフースとなっている。

したAP1は、APの公開職で暗号化したSTA のユーザ証 された公開鍵を用いて生成した共通鍵を暗号化する(ス アップS65)。そして暗學化した共通概を、認証ファ (4) 路局レフー464 元化十形代かなしたおり、Algo us Code 70-1-9, Status Code 70-2-9, St 四番10—3—3をAP1の路路機で復身化して、ST 今度は共通難を生成し、STA2のユーザ証明書に添付 ーム64を用いてSTA2に送信し、認配許可を通知す で、STA の公開機で暗号化した共通機70-4-3を付 加したフレームとなっている。なお、図2に示したStat atus Code 70-3-9 & UStatus Code 70-4-9 は、フレーム受信成功の可否などを通信相手に通知する A2のユーザ証明春の内容を検証し、STA2のユーザ **証明書の検証結果に問題の無いことを確認すると、次に** ritha Maber 70—4—1は哲治の通り「n」でもり、 る (ステップS66)。 路位フレーム64は、図1の Transaction Sequence Number 70-4-211 [4] 1

[0066] その後、ステップS66でAP 1から認証 フレーム64を受信したSTA2は、STA の公開録で時 れむの信仰レメーケドかわる。

整を使用することとなる(ステップS61)。 以上の動 引化した共通線70-4-3をSTA2の粉密機で復歩 比して、AP1が生成した共通機を復元し、この後実際 **に行われる無額通信におけるファーム暗号化に、蚊共通** 作により、公開難認証手順が終了となり、以後、STA 2とAP1間でフレーム暗号化通信が行われることとな [0067] 次に、再路配が行われる際の公開職再認能 年間について、図8及び図9を参照して説明する。

 図9は、公開機再級駐手頃において送受信されるM ACソフームのファームがディ的(区3のFraneBody 3 [0068] 図8は、公開録再認証手順を示す図であ 0-3)を示す図である。

再路信要状としてAP1に対して怒信ファー481を泌 [0069] <u>図8</u>において、昭和要求先のAP1に対し ムボゲィ郎は、図9の(1)昭和フレーム81に示す形 **-2を「1」としたフレームとなっている。なお、公開** 離再認証手順における認証時には、Algorithm Number 9 0-1-1~80-2-17年に「m」(mは「0」と 「m」とすることにより、<u>図6</u>に示した公開機器配手順 育する (ステップS81)。 路位フレーム81のフレー 男) 90-1-1を「m」とし、Transaction Sequence に過去に公開機器配発丁実機のあるSTA2は、公開機 Number (トランチケツョンツーケンス物本) 90-1 式となっており、Algorithm Marbor (アルゴリズム物 (1)と「n」でない午後の数) であるものと定職す 5. Algorithm Number 9 0-1-1~9 0-2-1全 と区別することが可能となる。

鬼怒した場合には、AP1は当該STA2に対して指定 アーブル40のPublic Ker40―2から取得した公開機 2―1は哲様の通り「m」であり、Transaction Sequen 早代した蛇共通戦90-2-3を左右したアレームとな っている。なお、図9に示したStatus Code 90—1—)及tVStatus Code 90-2-9は、フレーム受信成功 [0010] ステップS 8 1でSTA 2から公開競再認 に示した公開機管理デーブル40において、公開機再認 iddress 40-1に存在するが後報を行う(ステップS 82)。 そした、検索が成功し、かつ、それに対応する 公開鍵をPublic Key4 0 — 2 の描に保持していることを する共通鍵を新たに生成し、この新共通鍵を公開鍵管理 (当該STA2の公開機)を用いて暗号化する (ステッ **がS83)。 そして、暗写化した雑共通観を、認覧ファ** 4) - 路筒アアー482は、図96 (2) 路筒アアー4 8.2 に示す形式となっており、Algoritha Naber 9.0ー ce Number 90—2—2は「2」で、STA の公開館で掲 の可否などを通信相手に通知するための情報フィールド 旺要求を受信したAP1は、AP1が保持している<u>図4</u> 征要求を送信したSTA2のMACTドレスがSTA Mo ーム82を用いてSTA2に送信する (ステップS8

4暦号化に、政新共通轍を使用することとなる(ステッ [0011] その後、ステップS84でAP1から昭配 号化した新共通数90-2-3をSTA2の保持する秘 密難で復号化して、AP1が新たに生成した新共通観を プS85)。以上の動作により、公開競再路位手順が終 Tとなり、以後、STA2とAP1間でフレーム暗号化 フレーム82を受信したSTA2は、STA の公開機で暗 復元し、この後実際に行われる無機通信におけるファー 画信が行われることとなる。

【0072】以上、本地既の第1の実権形態について辞 冊に説明した。第1の実施形態においては、AP1とS FA2が共に自らの秘密機とそれに対応する公開録、及 **匹男者は邸症機関に代表される第三者によって公開艇と** その保有者との関係及び保有者自身の正当性を証明可能 公開機器証要求を行い、AP1から認証許可を得るまで 別に通びき、AP1とSTA2が認配的T供権のある相 り、2回目以降の認配要求時において四里に示す公開職 び公開録を添付したユーザ配明権を保持し、当該ユーザ であるという条件のもとで、STA2がAP1に対して こは、図6に示す公開機の交換年頃が発生するが、本発 再器証手順を用いることにより、初回の器証手順で行っ とで、認証処理手順の簡略化が可能となる、という効果 たAP1とSTA2関での公開線交換手順を省略するこ 年の公開整情報を認証解除後も保持し続けることによ を有している。

る路路敷に対応した公開敷によって暗中化するため、成 面観を取得することができず、従って本発明によって不 おいてユーザ証明書を用いることにより、AP1はST A2の公別機とその保有者であるSTA2の正当性とを 施路した上での認証許可後にSTA2の公開機情報を保 に対して送信する共通概を正当なSTA2のみが保持す りすましによる再認配要水元STAはこれを復身化し共 [0073] また、図6に示す初回の公開機器配手頃に 図8に示す公開機再認証手順を行うAP1は、STA2 Pすることから、当該STA2のMACアドレスを使用 した成りすましによる再認証要求が発生した場合には、 正なSTAによる成り丁ましを防ぐことが可能となる、 という効果を有している。

【0074】次に、本処界の第2の実権形態についた既

る構成は、例えば、複数のAPを統括する上位APを配 数し、上位APが公開機管理情報を一括して保持してお し、且つ各BSS同士が有機又は無線で接続される複合 ネットワーク上において、各APに帰属中のSTA (移 **影響末局)に関する公開整管理情報(具体的には、<u>図4</u>** ク内における共有情報とする構成とした無線LANシス アムである。複合ネットワーク内における共有情報とす に示した公開襲管理テーブル40)を、複合ネットワー [0075] 第2の実施形態は、複数のAP (基地局) による複数のBSS (基本サービス・セット) が存在

き、各APは必要時に上位APに対する登録あるいは間 い合わせを行い、その回答を上位APから得る構成であ 5. このような構成とすることにより、任意APに帰属 PのSTAが、BSSの体制により他のAP~初回の公 開戦認証を行う際にも、本発明による公開機再認証手順 を実施することにより認証処理手項の簡略化が可能とな 5、という効果を有するものとなる。

[0076] 太に、本発明の第3の実施形盤について設

[0077] 類3の実施形態は、IEE802.11で定機する

ところのIndependent (インディペンデント: 強立) 方 構成とすることにより、2回目以降の公開機再認証処理。 手頃の簡略化が可能となる、という効果を有するものと 式の無線LANシステムに第1の実施形態の本発明を適 て、IBSS内におけるSTAMでの公理機関的事にお でた、本部町の第10寅相形物に組むむ、公開戦略配限 **水を受信したSTAが認証要求元STAの公開録管理情** 0) を保存し続ける構成としたものである。このような (Independent BSS :インディペンギントBSS) 内に 用する構成である。Independent 方式では、IBSS 数数のSTAだけが存在し、APは存在しない。そし 線(具体的には、四4に示した公開整管理アーブル4

[0078] なお、本発明の第1、第2及び第3の実施 形態において、認配許可を行うBSS内APや1BSS 内STAが保持する認証要求元STAに関する公開機會 単価値の共に、ユード間配値に拠りへた名割配信を必要 入することによって、公開観管理情報の保持期限を持た せる構成とすることにより、有効が限切れユーザ配明値 の継続使用を防ぐことが可能となる。

認証手順の同時実現を可能とすることができるので、初 欧百姓研役の四一AP(独地略)に対する2回目以降の [発明の効果] 以上説明したように、本発明の無據LA Nシステムにおける認配方法と認配装置は、無鉄通信を 行う当事者間でのみ銘度性を保持した暗号用の観覧法と 回の昭配を治丁したSTA(移動端末局)に関しては、 80証手頃の簡略化を実現可能とする、という効果を有し

Cいる。 【図面の簡単な説明】

[図1]本発明の無機LANシステムにおける認配装置 [図2] APとSTAの一例を示すは描ブロック図であ と一段植形類やボナブロック図らせる。

[図3] 昭証要水時にAPとSTA間で治受信されるM

|図4| APが保持する公路整御理アーブルを収明する ACフレームの構成を収別する図である。 MARSON.

[<u>図5</u>] STAが保持するAP信仰管理アーブルを説明 rる図である。

9

9

*) } ;

特別2003-5641

(12)

体製2003-5641

Ξ

Ethernet (イーサネット)

BSS

[<u>図7</u>] 公開戦器駐手順において送受信されるMACフ

レームのフレームボディ部を示す図である。 [四6] 公開機器配手順を示す図である。

[符号の説明] 1 AP

てある.

)

(図3)

(13)

